Claims

What is claimed is:

1. A method for use in an RFID system comprising at least one RFID device and at least one reader which communicates with the RFID device, the method comprising the steps of:

associating a plurality of pseudonyms with the RFID device; and

transmitting from the RFID device different ones of the pseudonyms in response to different reader queries of the RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

2. The method of claim 1 wherein the transmitted pseudonyms are authenticated by the reader.

3. The method of claim 1 wherein the transmitted pseudonyms are authenticated by a verifier other than the reader.

4. The method of claim 1 wherein the RFID device is configured to authenticate itself to a verifier only after the verifier has authenticated itself to the RFID device.

5. The method of claim 4 wherein the verifier authenticates itself to the RFID device by releasing to the RFID device an authentication value β_i unique to a given pseudonym α_i transmitted by the RFID device.

6. The method of claim 4 wherein the RFID device authenticates itself to the verifier by releasing to the verifier an authentication value γ_i unique to a given pseudonym α_i transmitted by the RFID device.

7. The method of claim 1 wherein one or more of the pseudonyms each comprise an identifier of the RFID device.

8. The method of claim 1 wherein one or more of the pseudonyms each comprise a portion of an identifier of the RFID device.

9. The method of claim 1 wherein the pseudonyms are stored in the RFID device as an ordered list of pseudonyms, the method further including the steps of designating a particular one of the pseudonyms as a current pseudonym and, in response to a given reader query, transmitting the current pseudonym, wherein over a plurality of reader queries the pseudonym designated as the current pseudonym periodically cycles through the list of pseudonyms.

10. The method of claim 9 wherein after the current pseudonym is transmitted by the RFID device responsive to the given query, a different one of the plurality of stored pseudonyms is designated as the current pseudonym to be transmitted responsive to a subsequent query.

11. The method of claim 1 wherein one or more of the pseudonyms are generated on an as-needed basis within the RFID device.

12. The method of claim 1 wherein one or more of the pseudonyms are generated externally to the RFID device.

13. The method of claim 1 further including the step of limiting a rate at which the RFID device is permitted to transmit pseudonyms responsive to reader queries.

14. The method of claim 1 further including the step of periodically altering one or more of the plurality of pseudonyms.

15. The method of claim 14 wherein the altering step is implemented responsive to receipt of refresh information in the RFID device from a verifier.

16. The method of claim 15 wherein the refresh information comprises one or more refresh values transmitted from the verifier to the RFID device after mutual authentication of the RFID device and the verifier.

17. The method of claim 1 wherein for a given value κ utilized in the RFID device, a vector $\Delta_\kappa = \{\delta_\kappa^{(1)}, \delta_\kappa^{(2)}, \ldots, \delta_\kappa^{(m)}\}$ of one-time pads is maintained in the RFID device, wherein the one-time pad $\delta_\kappa^{(1)}$ is designated as a live pad and is used by the RFID device to update the value κ, where m denotes a number of authentication sessions over which one-time pads are constructed.

18. The method of claim 17 wherein the value κ is updated by computing $\kappa \leftarrow \kappa \oplus \delta_\kappa^{(1)}$.

19. The method of claim 17 wherein in conjunction with updating the value κ, the vector Δ_κ is updated utilizing a vector $\widetilde{\Delta}_\kappa = \{\widetilde{\delta}_\kappa^{(1)}, \widetilde{\delta}_\kappa^{(2)}, \ldots, \widetilde{\delta}_\kappa^{(m)}\}$ of one-time pads, the vector Δ_κ being updated by discarding the previous live pad $\widetilde{\delta}_\kappa^{(1)}$, setting $\delta_\kappa^{(i)} = \delta_\kappa^{(i+1)}$ for $1 \le i \le n-1$, setting $\delta_\kappa^{(m)} = 0^l$, and performing an element-wise exclusive-or of Δ_κ and $\widetilde{\Delta}_\kappa$ by computing $\delta_\kappa^{(i)} = \delta_\kappa^{(i)} \oplus \widetilde{\delta}_\kappa^{(i)}$, such that the updated vector Δ_κ comprises a set of m one-time pads with decreasing levels of backward secrecy.

20. The method of claim 1 wherein a verifier of the system is configured to store for a given RFID device T_x a static identifier id_x corresponding to at least one pseudonym of T_x.

21. The method of claim 20 wherein the pseudonyms for T_x are obtained by encrypting $id_x \parallel z_x$ under a symmetric key K_a for the verifier, where z_x comprises a pseudonym counter.

22. The method of claim 21 wherein when the verifier receives a pseudonym from the RFID device, the verifier decrypts the pseudonym using K_α to obtain the corresponding static identifier id_x.

23. The method of claim 1 wherein a verifier of the system in conjunction with an authentication session with the RFID device specifies a value identifying a particular pseudonym to be transmitted by the RFID device.

24. The method of claim 1 wherein the RFID device determines which of the plurality of pseudonyms to transmit responsive to a given reader query based at least in part on timing information.

25. The method of claim 1 wherein the RFID device incorporates a pseudorandom number generator, where $f_{\kappa_x}(i)$ represents an output of the pseudorandom number generator for index i, where κ_x is a seed associated with the RFID device.

26. The method of claim 25 wherein the RFID device generates the plurality of pseudonyms as pseudonyms $\alpha_1 = f(1)$, $\alpha_2 = f(2)$, ..., $\alpha_k = f(k)$.

27. The method of claim 25 wherein the RFID device and a verifier of the system attempt to maintain a common counter d_x unique to the RFID device, and share the seed κ_x.

28. The method of claim 27 wherein in order to determine which RFID device is associated with a given incoming value α, the verifier performs a lookup in a list $\{f_{\kappa_x}(d_x)\}$ of current α values for a plurality of RFID devices.

29. The method of claim 27 wherein for a given counter value d, the RFID device computes $a_d = f(bk + d)$, where b denotes a base value, and the verifier provides a subsequent instruction to the RFID device to increment the base value b.

30. An apparatus for use in an RFID system, the apparatus comprising:

an RFID device having a plurality of pseudonyms associated therewith and being operative to communicate with one or more readers of the system;

the RFID device being further operative to transmit different ones of the pseudonyms in response to different reader queries of the RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

31. An RFID system comprising:

a plurality of RFID devices; and

a plurality of readers which communicate with at least a subset of the RFID devices;

wherein a plurality of pseudonyms are associated with a given one of the RFID devices, the given RFID device being configurable to transmit different ones of the pseudonyms in response to different reader queries of the given RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

32. An apparatus for use in an RFID system, the apparatus comprising:

a reader which communicates with one or more RFID devices;

wherein a plurality of pseudonyms are associated with a given one of the RFID devices, the given RFID device transmitting different ones of the pseudonyms in response to different reader queries of the given RFID device;

wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

33. A method for use in a system comprising at least one device and at least one reader which communicates with the device, the method comprising the steps of:

associating a plurality of pseudonyms with the device; and

transmitting from the device different ones of the pseudonyms in response to different reader queries of the device;

wherein the pseudonyms are determined utilizing an updateable set of one or more one-time pads maintained in the device.